REMARKS

Favorable reconsideration of this application as presently amended and in light of the following discussion is respectfully requested.

Claims 1-30 are pending in the present application. Claims 1, 12, 19, and 30 are amended by the present amendment.

In the outstanding Office Action; Claims 1-3, 5, 14, 15, 18-21, 23-26, 29, and 30 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 6,337,712 to Shiota et al. (hereinafter "Shiota"); Claims 4, 6-9, 11-13, and 22 were rejected under 35 U.S.C. § 103(a) as unpatentable over Shiota in view of U.S. Patent No. 6,606,451 to Honda et al. (hereinafter "Honda"); Claims 16, 17, and 27-28 were rejected under 35 U.S.C. § 103(a) as unpatentable over Shiota in view of U.S. Patent No. 5,987,469 to Lewis et al. (hereinafter "Lewis"); and Claim 10 was rejected under 35 U.S.C. § 103(a) as unpatentable over Shiota in view Honda and further in view of Lewis.

Addressing now the rejections of all claims, summarized above, as anticipated by or as unpatentable over Shiota, those rejections are respectfully traversed.

Amended Claim 1 is directed to a filing system in which at least one data processing apparatus is connected to a file server via a transmission path. The filing system includes a data capturing unit, a data storing unit, an authorized user identifying unit, an access management unit, and a data output unit. The authorized user identifying unit acquires a ***plurality*** of owner identifications when image data is captured by the data capturing unit. The access management unit correlates the owner identifications with the image data stored by the data storing unit, and allows the stored image data to be accessed when any of the owner identifications correlated with the image data are verified. Amended Claims 19 and 30 recite similar features.

By way of background, image data may be shared by placing the data on a file server accessible by remote individual stations (Specification, page 2, lines 19-22). For example, scanned images may be exchanged amongst authorized users by accessing the server through their personal computers (Specification, page 2, line 24-page 3, line 4). However, when the number of images to be exchanged amongst authorized users is large, such a system becomes time consuming and burdensome (Specification, page 3, lines 5-8). Further, the contents of documents having confidential data (*e.g.*, passwords for file access) may be revealed during image capturing (Specification, page 3, lines 10-13). In view of these problems, the claims as currently written provide an apparatus and method for use in an image data filing system, whereby the identifications of selected authorized users are affixed to image data before transfer to a storage media, such that the stored image data are subsequently accessible by any of the authorized users by virtue of those attached identifications (Specification, page 3, line 23-page 4, line 6).

In a non-limiting example, Figure 10 illustrates an image data capture process of the present invention (Specification, page 34, lines 1-2). As shown, when image capturing is started, a processor reads the authorized user identifications ("IDs") provided from the results of the user ID acquisition process (Specification, page 34, lines 8-16). The user ID acquisition process may entail, for example, selecting (*i.e.*, acquiring) the multiple authorized user IDs by depressing respective buttons on a touchpad (Specification, page 33, lines 10-18). After the image is captured, it is determined whether all desired authorized user IDs have been acquired (Specification, page 35, lines 5-7). If so, an information file containing the authorized user IDs is created and added to the image data file (Specification, page 35, lines 13-17). Thus, after the image data capture process of Figure 10 is completed, both an image data file (containing the acquired image data) and an attached user information file (containing the authorized user IDs) are stored to the storage medium of the file server (Specification, page 36, line 20—page 37, line 1).

In another non-limiting example, Figure 13 illustrates the image data access process of the present invention (Specification, page 40, lines 24-25). As shown, before accessing the stored image data, the owner ID of the user seeking access must be authenticated (Specification, page 41, lines 10-14). Only a requesting user that has an authenticated owner ID (*e.g.*, matching one of the authorized user IDs attached to the desired image data) can retrieve the stored image data and reproduce/transmit the original image file (Specification, page 42, lines 19-22). Accordingly, the present invention provides increased availability of image data to multiple persons, while ensuring the security of such image data (Specification, page 42, line 23-page 43, line 4).

The outstanding Office Action cites Shiota as teaching Claim 1. More particularly, the Office Action cites an "identification code" of Shiota as teaching the claimed owner identification of the present invention (Office Action, 10/24/2003, page 3; citing Shiota, col. 10, lines 44-45). However, Shiota does not teach a system in which a ***plurality*** of owner identifications are attached to an image data file, such that the stored image data may be securely accessed and utilized by any user having an owner identification correlated to same.

Rather, Shiota teaches a system in which the image data recorded by a digital camera (and stored in a removable medium thereof) may be transferred to an image server for subsequent access, so that memory of the digital camera can be freed to store more pictures (Shiota, col. 1, line 64-col. 2, line 4; col. 2, lines 33-40). Shiota discusses the association of certain information with the transferred image data. For instance, Shiota mentions assigning a file name based on a camera code identifying the digital camera used to record the image; a possessor code representing the possessor of the digital camera; and a date code representing the date of recording (Shiota, col. 3, lines 41-46). Shiota also mentions the automatic association of ***an*** identification code with the image data (Shiota, Claim 33). However, none of those features teaches or suggests a system in which ***multiple users*** may have separate and secured access to the image data. Presumably, even if Shiota provided a system for attaching a password to the stored image data, the password would have to be disclosed to all persons seeking access. Such persons might also gain access to any other image data correlated with the password of the camera owner. Alternatively, multiple passwords might need to be created for respective multiple sets of image data, and the passwords distributed to all respective authorized users. These examples highlight some of the very burdens and security problems that the claimed invention avoids.

Accordingly, it is respectfully requested the rejections of independent Claims 1, 19, and 30, and the claims depending therefrom, be withdrawn.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance, and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Surinder Sachar

Gregory J. Maier
Attorney of Record
Registration No. 25,599

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/03)

GJM/SNS/STD/mac
I:\ATTY\STD\0557-4782\0557-4782.AM.DOC